

APL fully supports the National Maritime Security Advisory Committee (“NMSAC”) Recommendations on Developing a Contactless Biometric Specification for the Transportation Worker Identification Credential dated February 28, 2007 including Appendix II and III.

We especially support NMSAC’s recommendation on (1) the elimination of any use of PINs and (2) protecting the fingerprints through the use of a template in lieu of the use of encrypted finger-print images.

The use of pins and/or the use of encryption will make transaction times longer and increase cost with no improvement in security. The unintended consequence of the pin and /or encryption could actually degrade security and exacerbate adverse environmental conditions in and around port areas. For example, diesel exhaust will increase as a result of longer truck idling time. The exhaust contains particulate matter, a carcinogen and nitrogen oxides. This exhaust is a hazard for both the drivers and the surrounding community.

Finally, we do not support the “Alternate Option” described in Appendix IV as it would add costs and complications with no increase in security.

APL has been a strong supporter of the Transportation Worker Identification Credential (“TWIC”) program and has spoken publicly in support of this program. Our participation in the TWIC pilot program from the inception through the planning, technology evaluation and prototype phase ending June 30, 2005 also demonstrates our commitment to this important program.

We, however, wish to emphasize that DHS should continue to practice its twin goals of improving security while not crippling trade. Without balancing these two goals the danger of actually crippling the economic system we are trying to protect becomes probable.

TWIC should be viewed as one more important layer of security helping reduce the overall threat related to access. TWIC should not be seen as the silver bullet in making our ports more secure.

In this context, MTSA compliant marine facilities are already relatively secure. For example, the facilities:

- Have facility security officers overseeing all security efforts
- Have security assessments and detailed plans reviewed and approved by the USCG
- Conduct quarterly drills and annual exercises usually supervised by the USCG and others
- Have access control procedures in place
- Conduct screening of visitors and vendors as prescribed in their security plan
- Have CCTVs installed monitoring portions of the facility
- Undergo annual audits by the USCG

- Conduct security awareness training for all employees
- Receive ongoing visits by both USCG and CBP

Making this biometric identification card too complicated by selecting encryption and/or requiring the use of PINs will have adverse environmental impacts, increase stress on the already strained infrastructure, add to the trucker shortage and generally slow down the supply chain making the U.S. less competitive without improving the security of U.S. ports.

APL submits the following in response to the specified questions.

1. Should additional security measures be included in the specifications, such as the use of a PIN, to further minimize the chance that a fingerprint template from a lost or stolen credential could be obtained by an unauthorized individual? If so, would the addition of a PIN or other security measure adversely impact operations? Does the length of the PIN affect adverse impacts in any measurable way?

APL believes that requiring transportation workers to enter a PIN each and every time they enter a marine facility is unrealistic, does not provide added security given the degree of difficulty of this exercise and will adversely impact the flow of trade. We believe this is true regardless of the PIN length.

The following points are made regarding the challenges of the PIN:

- A large facility can have approximately 1,000 transportation workers on the premises at any given time. The majority of these workers will be entering and exiting the facility at approximately the same time for shift starts, meal hours and shift terminations. It is unrealistic to expect so many transportation workers (i.e., employees) to enter a PIN each and every time.
- The PIN is just one more “password” to remember and likely one more “password” that will be written down on a piece of paper that can be lost or stolen.
- Many transportation workers will create PINs that represent something easy to guess such as a birthday or phone number. We question the security value given this likely practice.
- Imagine a right handed trucker swiping the TWIC with his left hand, entering his PIN with his left hand and placing his left finger on the TWIC reader while his truck is idling at the marine gate.
- Not all transportation workers are adept at punching in numbers. Retrys will significantly delay longshoremen, truckers and/or other transportation workers.

In that each transportation worker will swipe a TWIC card and have that card authenticated with a finger print template, we see no benefit in requiring a PIN.

2. What, if any, privacy concerns exist if the fingerprint template is obtained by an unauthorized individual?

We have no privacy concerns if the fingerprint template is obtained by an unauthorized individual. We are told that reverse-engineering the template back into a fingerprint is impossible. Additionally, in our opinion, the finger print is not deserving of the same level of security as other personal data such as a social security number might require.

We completely agree with NMSAC's rationale as contained on pages 2 and 3 of their recommendations ("Privacy and Security Considerations.")

More specifically the recommendation states:

"Since only a fingerprint template will be passed between the card and the TWIC reader, the information cannot be reverse-engineered to a full fingerprint image.

Even if the template were "stolen" during contactless transmission to a TWIC reader, and even if somehow it could be used to replicate the original fingerprint, for which we understand no technology currently exists, the "thief" would not be able to use this illegal TWIC as the fingerprint image would not match his own when presented to a biometric reader in conjunction with a TWIC.

In addition, an individual interested in "stealing" a fingerprint would meet much less technical resistance and obtain a more accurate representation by lifting it from an object in a public place such as a car door, window or drinking glass."

3. How would the recommended specifications impact facility and vessel security and operations?

The recommended specifications, contained in Appendix III, would have minimal impact on facility and vessel security and operations.

However The "Alternate Option", contained in Appendix IV which requires encryption would have significant adverse impact on operations and security.

More specifically encryption adds significant complications. The biometric would remain encrypted during the transmission to the reader over the contactless interface. This requirement results in the need to decrypt the

biometric using the TWIC Privacy Key (“TPK”). Three alternative means are suggested to derive the TPK.

1. A magnetic stripe encoded on the TWIC card
2. The TWIC card memory
3. The physical access control system where it has been pre-registered.

The alternative of swiping the TWIC card through a magnetic stripe reader introduces the requirement for users to present the card to multiple sensors. The time required to swipe a magnetic stripe will push the transaction time beyond the recommended acceptable limit of three seconds.

These longer transaction times may:

- Increase the idle and queue times at the marine in-gate with trucks lined up on public roads creating health and safety problems.
- Increase congestion at the marine out-gate
- Delay vessel load/unload operations while longshoremen report to work
- Delay vessel and train schedules
- Increase vessel port time
- Require vessels to consume more fuel as they would be required to increase their speed to make up for lost time.

The above impacts will have adverse environmental impacts, increase stress on the already strained infrastructure in the U.S. and generally slow down the supply chain unnecessarily both for U.S. imports and U.S. exports.

Both the swipe of the magnetic stripe and the use of the TWIC card memory as alternatives to derive the TPK require the use of a contact interface. APL’s experience in operating marine terminals has resulted in abandoning the use of any equipment requiring slots such as a contact reader. In the marine terminal environment, these slots make the equipment vulnerable to sabotage, jamming and susceptible to environmental elements such as salt, dust and water.

When compared to the contact-less reader successfully tested in the TWIC pilot, the contact reader is:

- Prone to errors (card is inserted incorrectly)
- Less reliable (dirt accumulation in the card reader’s slot)
- More susceptible to sabotage (foreign object inserted in card reader slot)

A consequence of choosing a less reliable system subject to sabotage is that the facility owner/operator will need to rely on less effective back-up procedures in order to keep the facility operating and trade flowing.

Undoubtedly these “work around” procedures will not be as secure as the primary TWIC system.

The option to derive the TPK from the facilities Physical Access Control System where each potential user would be pre-registered would require a data base interface with the TSA. The details regarding this interface between the TSA and the owner/operator data base are unclear making it difficult to provide comments.

4. How would the recommended specifications impact existing physical access control systems?

The recommended specifications in Appendices III and IV would require that the existing physical access control systems at APL’s marine terminals be replaced and upgraded to TWIC Compatible Access Control Security Management Systems.

5. Are there alternative designs we should consider, and if so, what are the advantages and disadvantages of the alternative designs?

APL cannot determine the advantages/disadvantages of alternative solutions until detailed technical approaches regarding physical implementation are determined (eg, network, platform, configuration, hardware maintenance, software maintenance, etc)

6. How would the recommended specifications impact product, system, and operational costs?

The recommended TWIC Reader Hardware and Card Application specifications in Appendices III and IV would require that the existing physical access control systems at APL’s marine terminals be replaced and upgraded to TWIC Compatible Access Control Security Management Systems.

Actual costs will largely depend on TSA/USCG policy issues (e.g., record keeping and MARSEC level access control requirements) and resolving the privacy issues.

7. How quickly could the recommended specifications be incorporated into the design and manufacture of access control equipment?

LEFT BLANK ON PURPOSE

8. Should there be a process for identifying a Qualified Products List (QPL) or other equivalent regime? If so, what is the most efficient and effective way of creating a QPL?

A QPL should be developed.